Gordon L. Gibby MS MD KX4Z
15216 NW 41st Avenue
Newberry, Florida 32669

July 30, 2019

Via ECFS
Marlene H. Dortch
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Notice of Ex Parte Submission, Petition for Rulemaking filed by Amateur Radio Station Licensee Ron Kolarik (K0IDT), RM-11831

Dear Ms. Dortch:

I submit this ex parte letter in response to **Ex Parte Letter, dated July 24, 2019, by Theodore S. Rappaport, N9NB , Michael J. Marcus, N3JMM , Ari Q. Fitzgerald , and John W. Castle**.

Dr. T. Rappaport and his co-authors' elaborate *ex parte* filing[1] unfortunately appears quite flawed. The group (referred to here as "Filer") appears

1. unaware of recent data and impressive conclusions gathered on amateur radio self-monitoring and self-policing, incorrectly recognizing the significance of the data gathered and submitted in a recent filing by other proponents of RM-11831;
2. unaware of recent developments in Winlink Development Team ("WDT") software enforcement of various FCC regulations;
3. unaware of ARRL teaching, amateur discussions and issues related to the "control operator" issues;
4. intent on continuing a deceptive discussion tactic for which he has already been rebuked by a world-class expert;
5. to rely on flawed analyses by fellow proponents of RM-11831 of experiments already conducted;;
6. to advocate a flawed 3rd party management system that might seriously damage important communications between disaster-deployed amateur radio operators and state and local officials

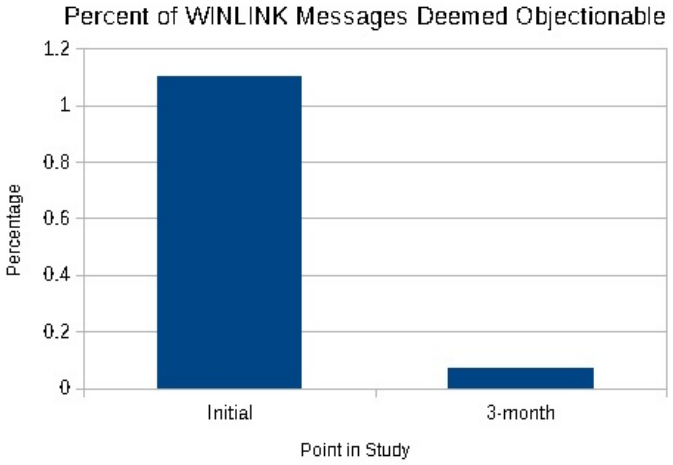
But the most confusing part of the filing is the area that it leaves completely **silent**: *Why the Filer hasn't already solved monitoring demands, to Filer's own satisfaction, given Filer's great expertise and resources, if Filer continues to reject the largest freely available, distributed receiver ever created, and available for Filer's pleasure.*

Finally, the Filer seem completely oblivious of how much damage would be done to Filer's own stated objectives if Filer's prescriptions were followed.

1 https://ecfsapi.fcc.gov/file/10724035705944/NYU%20Ex%20Parte%20Filing%20-%2007.24.19.pdf

Area	Claims by the Filer	Response
1	The Filer repeats the same basic claims on **non-observability and unchecked violations** multiple times throughout: [emphases added in quotes below] "Amateur operators and members of the general public are unable to decode Winlink messages over-the-air for true meaning and, in many cases, **are unable to determine where the rule violations are occurring, rendering real-time self-policing and rules enforcement impossible**. Meanwhile, Winlink's feeble and self-serving excuse for an enforcement mechanism has **failed to deter these rule violations** or give the amateur community the confidence that rules enforcement is even a Winlink goal. " "A complaint filed recently with the FCC's Enforcement Bureau demonstrates that gross violations of regular usage and business usage over the amateur bands have been occurring via the Winlink system for well over a decade, and continue to occur regularly, even after the establishment of a viewer" "Winlink's current excuse for an enforcement mechanism **has proven ineffective in preventing violations of the Commission's rules**, and an effective self-policing regime that ensures that amateur frequencies are used solely for non-commercial purposes requires the ability to decode over-the-air transmissions. " **"**The Winlink system's current excuse for an enforcement mechanism, which relies on use of the Winlink viewer, **has proven ineffective in curbing violations of the Commission's amateur service rules. "**	The Filer simply has not kept up with the rapid applicable progress of the last 3 months. Filer's claims made regarding ineffectiveness and lack of intent to improve compliance have been completely disproved in a filing by me, just days before Filer's filing. Filer's claims have been demolished, by objective results. . **There is actually no other portion of amateur radio which has any similar documentation not only of compliance rates, but of an astonishingly effective enforcement system!** (Completely the opposite of assertions the Filer repeats so many times.) The best data available to date (due to reluctance of the proponents of RM-11831 to provide complete data) demonstrate that the observed noncompliance rate with Winlink Terms and Conditions or FCC regulations was approximately 1.1% for the period of 21 days immediately prior to the institution of the WINLINK VIEWER. The Filer appears to misunderstand the data gathering techniques utilized by Carson et al.[2], who gathered their data in the first 12 hours of the existence of the WINLINK VIEWER (on or about April 10, 2019)[3] and therefore had access only to the 21 days of data *prior* to the VIEWER. The data the Filer references since that date is anecdotal data. The Filer appears completely unaware of significant new statistical data collected and analyzed since April 10, which demonstrates that the estimated non-compliance rate with the Winlink Terms and Conditions[4] had dropped by an astonishing amount, over 11 times, and in the most recent measurement was **less than 0.08 of 1 Percent.**[5] In evaluating these results, it must be recalled that the WINLINK Terms and Conditions are far more strict on business communications (the most commonly-cited issue) than the FCC's enforcement, as widely explained in the "Pizza Rule".[6] Thus, it is quite likely that even

2 https://ecfsapi.fcc.gov/file/1071958608259/July%2018%2C%202019%20Ex%20Parte%20Filing.pdf
3 Information helpfully provided by Petitioner (Ron Kolarik) https://forums.qrz.com/index.php?threads/arrl-report-no-consensus-reached-for-fcc-on-"symbol-rate"-issues.666183/page-30#post-5138180
4 https://winlink.org/terms_conditions
5 https://ecfsapi.fcc.gov/file/10723230403421/IncidenceCalculations.pdf

		the majority of the remaining 0.076 of 1 Percent issues are actually not even a violation of FCC Regulations. The following Figure[7] illustrates the dramatic reduction of violations of the WINLINK Terms and Conditions, from their already-low 1.1% initial measurement:  The Filer's assertions that compliance can not be determined, and that improvements are ineffective are completely *demolished*. Further, it is likely that many of the reports are being done by the compatriots of the Filer, so that the WINLINK system is being <u>effectively policed by persons with a vested interest in finding every possible potential violation</u>. It would be difficult to construct any better system for improving compliance.
2	The Filer is unaware of recent innovations created by the WDT in their manifest determination to assist the Enforcement Bureau and improve amateur radio: "Winlink's **current excuse for an enforcement mechanism** reveals that e-mails have traveled through the Winlink system that violate the third party	The Filer again relies on anecdotal data rather than statistical.[8] On July 20, 2019, four days before the July 24th filing by the Filter, this service message went throughout the WINLINK system to all users, reflecting a new advancement: Message ID: P0ZHC9LTBDZQ

6 "Calls to place an order for a commercial product may be made such as the proverbial call to the pizza restaurant to order food, but not calls to one's office to receive or to leave business messages since communications on behalf of ones employer are not permitted. " quoted from http://www.arrl.org/phone-patch-guidelines

7 Illustration from: https://ecfsapi.fcc.gov/file/10723230403421/IncidenceCalculations.pdf

8 For a comparison of the validity, see: https://statisticsbyjim.com/basics/anecdotal-evidence/

	restrictions. For example, in May 2019, a Norwegian amateur radio operator on a sailboat sent an e-mail to another sailboat through a U.S.-based Winlink gateway, despite there being no third party agreement between the United States and Norway. “ [emphasis added]	Date: 2019/07/20 22:18 From: W3QA To: [deleted] Source: SYSTEM Downloaded-from: Telnet:cms.Winlink.org Subject: US THIRD-PARTY MESSAGES RULES NOW ARE ENFORCED BY CMS All, If you are a US-licensed station that routinely connects to a foreign gateway, or a non-US-licensed station that connects with a US gateway, you may be affected by new CMS behavior. The Winlink CMS now will enforce US Third-Party Message rules. Because Winlink is being severely criticized for allowing US client and gateway operators to violate US amateur radio third-party traffic rules, we are today starting to test automatic enforcement of these rules. Part 97.3(47), 97.115 and 97.117 apply. If you attempt to send or receive a third-party message between a US-licensed station and another station the US does not have a third-party communication agreement with, you may receive a service message saying the message will violate the applicable rules and that the message is refused (if you're sending) or being held at the CMS (if you are receiving). Alternative means to successfully send or receive the message will be explained. The US has treaties with most countries in the North and South America, but not most European, Asian and Pacific countries. If you are a US-licensee, you should have no trouble sending and receiving to/from internet addresses if you connect with another US-licensed gateway, or one licensed in Central or South America ? as long as the US has a third-party agreement with the licensing country. If you are a non-US licensee, you should have no trouble sending and receiving to/from internet addresses if you connect to non-US licensed gateways. We wish this was not necessary, but we have relied on

		US client and gateway operators to know the rules and obey them and most have ignored them, unfortunately for all of us. In order to clean up the violations we are taking these measures to keep US Winlink operators legal. All licensees have an obligation to study, know, and obey the Amateur Radio Rules. New monitoring and enforcement measures are coming into play with the establishment of a new Volunteer Monitor Program, now being set up by the ARRL at the request of the US FCC. We're doing this to make it easier for US operators to avoid loosing their licenses! We will be tweaking the behavior of this new mechanism to make it as friendly and informative as it can be. Please bear with us as we make changes. Thanks and 73, Lor W3QA Winlink Development Team As might be expected, there will be adjustments as this new software is tested. To my knowledge there is no other portion of amateur radio where any automated enforcement of these regulations is occurring, making WINLINK the current innovation leader.
3	The Filer makes the common assumption that the control operator of a gateway station is the station licensee and then launches into a large number of conclusions based on that assumption. He make no mention of 6-year old ARRL teaching that contradicts his stance: *"47 C.F.R. § 97.115(b)(1)*, which requires that, with regard to third party communications, the "control operator [be] present at the control point and is continuously monitoring and supervising the third party's participation." Many of Winlink's control operators are not "continuously monitoring and supervising"	For a more complete discussion of this complicated issue, Filer would have necessarily provided the text present in both the 10th and 11th Editions of the <u>ARRL Extra Class License Manual</u>, which directly contradicts his assertions, and then provided a discussion of how to balance his viewpoint versus that published in ARRL texts: <u>The ARRL Extra Class Manual</u> Chapter 3, Rules and Regulations Subsection REMOTE CONTROL *"It is important to be aware of the rules for remote control because more and more radio equipment is designed to support remote control. A popular example of stations under remote control are the digital Winlink RMS PACTOR stations*

	to determine whether third party participation complies with the amateur service rules. Instead, these control operators are relying on automatically controlled digital stations ("ACDS"), which send e-mail messages over the amateur bands that may violate the Commission's rules. ¸ *47 C.F.R. § 97.105(a)*, which requires that control operators ensure "the immediate proper operation of the station, regardless of the type of control." Failure to comply with Section 97.115(b)(1) also leads to violations of this more general provision. "	*9www.winlink.org) that wait for a station to call them before responding. The RMS station is considered to be remotely controlled by the controlling operator"*[9] This topic was fervently discussed on a recent national amateur radio forum including the Petitioner[10] and other proponents of RM-11831. The Filer seems unaware of the facts and issues brought out in that discussion. There are issues on both sides of the discussion of who, precisely, is the control operator of a RMS Gateway.[11] It is quite likely that innovation in this aspect, has gotten farther than FCC Regulations – an event that the FCC has repeated recognized in other settings and altered Regulation to provide for innovation.[12] In this case, if the Control Operator is in fact the amateur downloading a message, then they are in fact the person exerting a significant measure of control over the transmission of that potentially 3rd party message over amateur radio (not the station licensee of the gateway); thus the Filer's objections become moot as he addresses the wrong party. There are factors both in favor, and opposed to this ARRL interpretation: **In favor:** • The client amateur radio operator chooses the frequency of the communication. • The client amateur radio operator alone made the decision to allow the particular 3rd party to have access to the system – and the 3rd party can only communicate with the client amateur radio

9 The American Radio Relay League, The ARRL Extra Class License Manual, p. 3-10, c. 2012 The same text appears in the 11th Edition. Whether correct or not in the judgment of the FCC, this is what the ARRL chose to print.

10 Here and elsewhere, Petitioner refers to the writer of the Petition leading to RM-11831: https://ecfsapi.fcc.gov/file/100918881206/PETITION%20FOR%20RULEMAKING.pdf

11 "Control Operator" appears to be a historical legal construct for assigning sole responsibility for transmissions from a radio transmitter. Over time, remote control operator, and now "automated control" have been recognized as innovation and technology grew.

12 An example where the FCC recognized innovation was outstripping their regulations: "The rules adopted in this Report and Order will update the ERS to a more flexible framework to keep pace with the speed of modern technological change while continuing to provide an environment where creativity can thrive. To accomplish this transition, we are creating three new types of ERS licenses…." http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-13-15A1_Rcd.pdf and another similar acknowledgment of the need for regulation to be adjusted to accommodate innovation: https://web.cs.ucdavis.edu/~liu/289I/Material/FCC-03-322A1.pdf

		alone, not to others, as is the case with other portions of the amateur radio system. • The client amateur radio operator chooses the time. • The client amateur radio operator chooses whether to download the message or not (and thus exerts ultimate control on whether the message is transmitted over amateur radio). • The client amateur radio operator has the ability to stop transmissions by the gateway from the STOP feature of the software (but not instantaneous cessessation.) • These appear to fulfill the ordinary view of control of an amateur radio station. **<u>Opposed:</u>** • The client amateur radio operator cannot know the statement(s) made the 3rd party whom they approved until all the statements have been transmitted over the radio; whereas in a live situation over SSB the operator might have physically intervened to stop transmissions mid-stream • The client amateur radio operator does not have direct physical ability to stop the transmission, and is dependent on software remote control (but so are many remote control operators).[13] • The client amateur radio operator is exerting their degree of control over a radio link that is potentially on HF frequencies, which is not a suitable frequency for remote radio control.[14] • If the client amateur radio station is foreign-licensed, then it is an inappropriate remote control. This issue is complicated, and the innovation in amateur radio has obviously presented a confusing issue even to the ARRL text writers (and apparently unobserved for 6 years). **It remains for the FCC to present how this should be properly viewed, or modify regulation to more clearly accomplish regulatory goals.**

13 See for example, https://k6ufo.com/attachments/Remote_Op_Ten_Things.pdf
14 See §97.213, §97.201 and 97.3(7) [which does not include a message forwarding station.]

4	The Filer continues to utilize deceptive descriptions: The filing uses some variation on the word "encrypt" **thirty or more times,** attempting to make the case that the WINLINK system's usage of ARQ and compression is unlawful.	I would have no disagreement if the Filer had used perfectly straightforward wording such as "**difficult to reconstruct**" since there *is* a measure of engineering required to receive modern digital signals. Google searches for "effectively encrypted" produce articles on *how to use encryption more effectively to prevent intruders from ransomware or other attacks*! Nothing to do with amateur radio, or software compression. This is an invented term. If is obvious from examining the software of a working third-party open source Winlink client maintained by John Wiseman, that there is no encryption utilized in WINLINK, rather LZHUF compression is utilized to reduce time/bandwidth. **<u>The impacts of these two completely different technologies are totally different at every point:</u>** • Compression utilizes computer power to take advantage of statistical redundancy in clear-text material, to create an index that allows the clear text to be transmitted with fewer bits. Once received at the other end of the channel, computer power is required to convert back from the indexed information into the original text. There is no secret key, no private key, no public key – no cryptographic key at all. All of the information needed to read the message is transmitted with the message itself. • Encryption uses computer power and some secret (public or private key, or symmetric key) so that even if the data are received perfectly, the message cannot ever be reconstructed with practical limits on computer power --- and the cryptographic key must have been transferred by some other channel to only the intended recipient. • For compression, effort applied to obtain a more robust received signal will eventually

succeed, and indeed may be *more successful* than the intended (single-receiver) recipient! Adding additional receivers increases the odds that the monitoring system will actually have an easier time capturing the material, than the intended recipient.

- For encryption, it does not matter how much effort the monitor places into reception – they will never succeed in being able to view the data.

- For compression, ARQ retries BENEFIT the monitor.
- For encryption they don't provide any meaningful advantage.

- For compression, FEC inside the packets BENEFITS the monitor;
- for encryption, FEC doesn't solve the problem at all.

- For encryption – the problem is **insoluble**.
- For compression, the probably merely requires a **successful engineering solution** to obtain good data, because there is no fundamental reason why the text cannot be obtained.

The above contrasts strongly suggests that using any form of the word "encryption" is done with a specific intent to <u>change the understanding of the task facing the monitor</u> from one that is *possible*…. to a term that incorrectly connotes *impossibility*. This is a subtle deception.

Although the Filer never gives a concise definition of this new term "effectively encrypted," based on the multiple usages, a definition might be:

> *"Effectively Encrypted": Communicated using available public technology that has specific hardware and software requirements, as well as engineering hurdles which can be met, but require appropriate hardware and software to*

		read. The difficulty the Filer is having relates to the **failure to develop the necessary software to recover the available signals, beyond that freely provided by the WINLINK group for any and all users.** (The mystery of why this software has not yet been developed, despite Filer's technical expertise, vast available resources, and historically expressed concern for the security of the Nation is covered later.[15]) However, the WINLINK development team has assisted the Filer by providing a web-readable, 100% perfect copy of American-related messages. Filer and proponents of RM-11831 have demanded free systems to monitor WINLINK transmissions. The Winlink Development Team accomplished that in spades: These messages were actually received over the air, (as demanded by Filer) using publicly available software, by volunteer amateur radio operators, with perfect copy, and made available from their receivers to (at least) the entire amateur radio community—not just one or two individuals. ***Likely the World's Largest Distributed, Freely-Available, Networked, Over-The-Air Receiver[16]*** This constitutes **the world's largest, distributed, networked, hybrid, web-accessible, freely available, software-defined/hardware-based volunteer-operated, over-the-air Receiver.** It is based on an incredible amateur radio development, which has proceeded with acclaim for over 2 decade, but became a web-accessible vast over-the-air receiver on April 10, 2019. *All created and provided by volunteers for the Filer's pleasure to assist in the world's first objective demonstration of amateur radio compliance*

15 Filer stated in 2016: "I pointed out national security concerns with the current problem of encrypted data, which arises from the non published compression algorithms used in Pactor II, Pactor III, and Pactor IV, and also discussed how the identification of many ACDS stations are often encrypted, as well, since that is an option on the SCS modems. " https://ecfsapi.fcc.gov/file/1110241203910/Reply%20to%20Comments%20NPRM.docx

16 Every message capture by this Receiver was actually received over the air by a physical receiver, connected together in a vast distributed receiving system constituting a networked Receiver.

		improvement. Yet Filer inexplicably finds this software-based "receiver" with unmatched performance features, unacceptable. Undeterred by the creation of a system which largely fits Filer's goals, , the Filer employs deceptive wording for the apparent purpose of smearing the underlying system (in use for 2 decades) with the illusion of illegal operation. Filer makes no explanation why the Commission has allowed this blatant operation to go on for so many years[17], why the ARRL has often lauded it, many ARES communication plans include it, and operators were sent to Puerto Rico with the original plan of utilizing it![18] The engineering and legal reasons that 30-year-old LZHUF compression were chosen have already been thoroughly explained. [19] [20] [21] **The Filer makes no rebuttal to the facts presented.** The Filer was rebuked by a world-class expert already in formal FCC filings, for this improper terminology but this has made no discernible impact.[22] Should the Filer continue to eschew usage of this vast free distributed over-the-air receiver, constructing a diversity receiving system is advised. ARZ "repeats" by the intended recipient will actually add additional improvement to the monitoring station, and the embedded FEC within some protocols (notably PACTOR) will further enhance their success. Such diversity receiving systems are now already in common use by Contest monitors according to data provided by a League official.[23]

17 Filer boldly claims: 'This history underscores why other, more advanced and unpublished communications modes currently used by the Winlink system are prohibited under Section 97.113(a)(4). "
https://ecfsapi.fcc.gov/file/10724035705944/NYU%20Ex%20Parte%20Filing%20-%2007.24.19.pdf

18 Filer, in footnote 19, attempts to justify this by citing private assertions by other commenters, which comments do not even include the concepts of expert testimony.
https://ecfsapi.fcc.gov/file/10724035705944/NYU%20Ex%20Parte%20Filing%20-%2007.24.19.pdf

19 See historical and engineering discussion, pp3-5 in
https://www.qsl.net/nf4rc/2019/SpyingOnWINLINKV2.pd

20 See page 3 of https://ecfsapi.fcc.gov/file/10722131064325/REPLYtoCarsonExParteFilingProposal.pdf

21 For a simple explanation of LZ type compression/decompression, see:
https://www2.cs.duke.edu/csed/curious/compression/lzw.html

22 See p 2ff. https://ecfsapi.fcc.gov/file/10513525129724/rm11831-rebuttal-to-rappaport.pdf

23 https://forums.qrz.com/index.php?threads/expectation-of-privacy.666437/page-14#post-5140630

5	Rather than providing his own engineering analyses of available experimental data, the Filer relies on flawed analyses provided by non-professional observers in previous filings: *"See* Reply Comments of Ron Kolarik, RM-11831, at 1 (July 17, 2019) (discussing numerous flaws with attempted demonstration that sought to prove amateur users' ability to intercept Winlink messages over-the-air); *see also* Reply Comments of Professor Theodore (Ted) S. Rappaport, RM-11831, at 6 (Apr. 29, 2019) (Winlink's combined use of fading channels and "differential encoding or compression . . . [creates] secure, effectively encrypted communications.")." In the Filer's April 29th filing he stated: "However, HF radio channels undergo fading which causes the channel states to be different for an eavesdropper than for a particular transmitter or receiver engaged in a connected file transfer. By using ARQ on HF fading channels, combined with differential encoding or compression that uses the instantaneous channel state information shared between a specific connected transmitter and receiver to encode successive packet data transmissions during a connection, ARSFI/Winlink is able to obtain secure, effectively encrypted communications in amateur radio, since the specific channel states between a unique transmitter and unique receiver are used to encode the subsequent data bits of that transmission packet on each ARQ packet interlude, and that precise channel state used for the encoding of subsequent packets is generally different and independent from a random eavesdropper. "[24]	The Filer does not appear to understand that the WINLINK system **does not utilize internal PACTOR compression algorithms**, which might have channel state-dependent information. Instead, the WINLINK system utilizes LZHUF 30-year old public compression which has **no knowledge of the radio communication underway.** State information as to changing levels of speeds can be received by a monitoring station just as they would be received by the counter-party of a WINLINK exchange; with diversity receiving, the monitoring system would on balance have a greater chance of picking this up earlier than the single-receiver intended recipient. Thus these transmissions are laughably "secure." Indeed, our group carried out a special-circumstance monitoring of compressed winlink messages, five different times – <u>while carefully explaining the limitations and purpose of the demonstration</u>, and providing a completely separate chapter on how to build the monitoring system that the RM-11831 proponents demand. [25] Unaware of the actual technical compression systems, the Filer makes additional false claims: "*If an eavesdropper experiences a different channel state (e.g. has different fading conditions, which is certain to be the case over many packets) than the connected transmitter and receiver, the eavesdropper cannot fill in the proper information to intercept over-the-air data, since it is missing the precise channel state information needed to decode the successive transmissions properly. The eavesdropper sees gibberish, as has been reported widely for over a decade.* "

24 https://ecfsapi.fcc.gov/file/10429199250117/FCC%20Letter%20Reply%20to%20Comments%20RM%2011831.pdf

25 In great contrast to the writing of the Filer, see pp 5-9 of https://www.qsl.net/nf4rc/2019/SpyingOnWINLINKV2.pdf for a carefully explanation of the tasks to obtain the Filer's monitoring system, as well as the limitations and goals of the simple demonstration carried out without any code written.

		The obvious solution has been explained so that Filer can read it, in multiple locations.[26] Filer has made no rebuttal to the suggested design. **<u>Packet headers</u>** The content of the header packets and other information are described in published material available on the SCS web site. Some of that explanation is repeated here: *"Except from different data field lengths, the basic PACTOR-3 packet structure is similar to the previous PACTOR modes. It consists of a packet header, a variable data field, a status byte and a CRC. Two types of headers are used: Sixteen "variable packet headers" consisting of 8 symbols each are sent alternately on tones 5 and 12 to code 4 bits of information: Bit 0 defines the request-status indicating a repeated packet. Bits 2 and 3 specify the speed levels 1 to 4 according to a modulo-4 logic, whereas the detection of levels 5 and 6 is performed by additionally analyzing the constant packet headers. Bit 4 gives the current cycle duration: ....* *The remaining tones 1-4, 6-11 and 13-18 are preceded by constant headers that characterize the respective tones* ***without transferring any additional information****. They support frequency tracking, memory-ARQ, the Listen-Mode and the detection of the speed levels 5 and 6. Figure 6 presents the hexadecimal codes of the constant packet headers. "*[27] [emphasis added] While complicated, this information is handled by the receiving PACTOR modem and thus is unlikely to be a concern of the software developer. The SCS company has already explained that any of their modems has the ability to monitor other transmissions.[28] That should be obvious – amateurs use them for QSO's! How would they ever make contact otherwise? **<u>Understanding Digital Systems</u>**

26 See Chapter 1 https://www.qsl.net/nf4rc/2019/SpyingOnWINLINKV2.pdf or purchase here: https://www.amazon.com/dp/1080563199

27 https://www.p4dragon.com/download/PACTOR-3%20Protocol.pdf

28 "PACTOR monitoring mode is available in all our modems." page 3, https://ecfsapi.fcc.gov/file/10417301289214/SCS_FCC_Comment_RM11831.pdf

		The original Petitioner completely mixed up the characteristics of my single-purpose proof of concept demonstration, with the characteristics required to build a full monitoring system[29]; yet the Filer relies on their filing to dismiss what was an actual proof that there is NO encryption. It took quite a bit of writing to disentangle the erroneous statements[30] made by the Petitioner regarding the text that we published and is currently available on the web, as well as through commercial vendors. Our demonstration[31] proved that there is NO ENCRYPTION, and the remainder of a monitoring system is merely an ENGINEERING PROJECT – for which the Filer and his university department should have been well suited. Clarke's 3rd law states that any sufficiently advance technology appears indistinguishable from magic[32] – so perhaps the Filer's continued mis-characterization of WINLINK as "effectively encrypted" is a subtle way of admitting the technological advances of the WINLINK development so many years ago, to make efficient use of bandwidth/ time on amateur radio bands.
6	Advocating a flawed system of 3rd party communications that might seriously damage emergency communications "….Winlink should: (1) make all international and domestic e-mail messages and files traveling through its system available for inspection in real-time by the public *before* they are transmitted over amateur frequencies"	Here, an example demonstrates the flaws of the Filer's demands: Imagine the circumstance that a deployed amateur radio operator in a devastated area (such as Bay County, after Hurricane Michael just last year[33]) has enabled 3rd party email communication from the State of Florida emergency manager. As Tallahassee still has internet connectivity, the EM might well send bulletins or other information to deployed amateurs giving important directives and other information. The Filer's proposed system would force those messages to be inspected (perhaps even "by the public") before they are transmitted? So the volunteer at a shelter in Bay County, making a connection by generator power [our county had a team right there]

29 https://ecfsapi.fcc.gov/file/1071758880862/Reply%20to%20Gibby%20comments.pdf
30 See "2. Petitioner's Confusion" in https://ecfsapi.fcc.gov/file/10720527000059/RM11831-July20.pdf
31 https://ecfsapi.fcc.gov/file/1071540521688/FCCCommentJuly2019.pdf
32 https://en.wikipedia.org/wiki/Clarke%27s_three_laws
33 https://www.amazon.com/Hurricane-Michael-After-Action-Report/dp/1729341918

		would potentially miss the message from the State of Florida EM? And what is this considered an advance? Amateur radio operators potentially volunteering with the Florida Baptist Disaster Relief feeding teams and dependent on radio communications for orders of ingredients for up to 15,000 meals were day would be hindered in 3rd party communications with their Logistics Director (who is not yet an amateur). And this is an advantage? The proposed system is unwieldy and does not recognize that the amateur radio operator who has specifically authorized the 3rd party individual is the person taking the responsibility.[34] This is a very workable system, which the Filer does not seem to recognize.

There are surely many other claims made that *I simply can't get to*. Perhaps one of the most amusing is the claim that silent RMS gateway stations exert some "claim" on a frequency[35] – the Filer has apparently never listed to what happens during an RTTY contest! RTTY stations take full advantage of all lawful frequencies.

Why didn't the Filer just build it?

However, by far, the most confusing aspect to me is that the Filer, of all people, hasn't already created the very monitoring system believed necessary for national security [36]– if the Filer continues to reject usage of the vast, freely-available, distributed Receiver that the Winlink Development Team has constructed and made available expressly to accomplish the monitoring and enforcement goals expressed by the Filer. Filer's group includes an acknowledged radio communications expert[37], an accomplished amateur radio operator, a distinguished Professor at a prestigious university with many faculty and graduate students under his control.[38] The letterhead on which Filer's message is communicated obviously speaks of great resources. I would be better able to understand the position had the Filer reported specific experimental efforts and described specific technical issues that were encountered in scores of hours of testing. However, to date I have not seen any such material. I'd be delighted to learn from it, should it exist.

34 https://winlink.org/HELP

35 "The use of an ACDS to operate part of the Winlink system can cause the commandeering of certain amateur frequencies, effectively shutting out other amateur users and making exclusive use of the frequency." p6 of the Filing.

36 https://forums.qrz.com/index.php?threads/expectation-of-privacy.666437/page-11#post-5140239 and https://forums.qrz.com/index.php?threads/expectation-of-privacy.666437/page-14#post-5140629 and https://forums.qrz.com/index.php?threads/expectation-of-privacy.666437/page-15#post-5140656

37 https://wireless.engineering.nyu.edu/ieee-honors-ted-rappaport/

38 See extensive web site at: https://wireless.engineering.nyu.edu/

Furthermore, the Filer has spoken of a desire to attract young people to amateur radio. NYU is a large, and distinguished private university with over 50,000 students.[39] The Filer is in a perfect position to hold a competition with undergraduate or graduate students to complete the desired monitoring system – beginning with a simple system that works with favorable signal-to-noise ratios using one receiver, and then expands to multiple diversity receivers.

Further, the area immediately surrounding Filer is rich with talented persons. This would be a perfect opportunity to encourage persons interested in software development to dip their toes into amateur radio. Even a cursory search of the vast New York City area (searching for computing-related clubs within 25 miles) reveals well over 30 applicable clubs, including over 50,000 persons with an interest in the skills necessary to complete this project.[40]

I'm still busy in the practice of medicine, and our medical campus is quite removed from the engineering portions of the University of Florida, but after I retire, this is a project that might attract the interest of the local Linux club or similar. Or I might even have a crack at it!

Impact of Filer's Wishes

Finally, the world that the Filer proposes to create (should success be obtained in hobbling WINLINK) seems **far more disadvantageous to their stated objectives** than what now exists, and has been documented in filings with the FCC.

39 https://www.usnews.com/best-colleges/nyu-2785

40 https://www.meetup.com/topics/computer-club/us/ny/new_york/ returns the following:

CLUB	Members
https://www.meetup.com/NYC-In-Memory-Computing-Meetup/	1593
https://www.meetup.com/Amateur-Computer-Group-of-New-Jersey-ACGNJ/	681
https://www.meetup.com/Moad_Computer/	144
https://www.meetup.com/NY-Enterprise-Information-Security-Meetup/	4599
https://www.meetup.com/New-York-Quantum-Computing-Meetup/	895
https://www.meetup.com/NYC-BCI-meetup/	443
https://www.meetup.com/Greater-Westchester-Personal-Tech-and-Computer-Users/	141
https://www.meetup.com/nysoftware/	8999
https://www.meetup.com/nyacc_org/	549
https://www.meetup.com/Unigroup/	235
https://www.meetup.com/SemioticsWeb/	608
https://www.meetup.com/CSTA-NYC/	2259
https://www.meetup.com/IBM-Watson-Cognitive-Computing-Meetup/	647
https://www.meetup.com/Manhattan-CS-Community-of-Practice/	48
https://www.meetup.com/Bronx-CS-Community-of-Practice/	28
https://www.meetup.com/Brooklyn-CS-Community-of-Practice/	55
https://www.meetup.com/Queens-CS-Community-of-Practice/	50
https://www.meetup.com/Staten-Island-CS-Community-of-Practice/	33
https://www.meetup.com/Jersey-City-Computing-and-Engineering-Meetup/	103
https://www.meetup.com/Build-with-Code-New-York/	9388
https://www.meetup.com/Alluxio-Open-Source-New-York-Meetup/	189
https://www.meetup.com/DigitalOceanNYC/	4740
https://www.meetup.com/Practice-coding-problems-in-NJ/	150
https://www.meetup.com/Masters-in-Web-Dev-Data-Structures-Algorithm-Practice/	34
https://www.meetup.com/nyccloudcomputing/	1255
https://www.meetup.com/NYC4SEC/	599
https://www.meetup.com/OpenStack-New-York/	2292
https://www.meetup.com/hackmosaic/	1856
https://www.meetup.com/nyhacker/	8395
https://www.meetup.com/NYC-Codecademy-Group/	3057
https://www.meetup.com/Women-in-Cybersecurity-Information-Security-New-York/	380
https://www.meetup.com/NYC-Raspberry-Jam/	386
https://www.meetup.com/ACM-NY/	1723

The Filer wishes to remove ARQ and have WINLINK uses dispense with compression and use Forward Error Correction systems. While these are very useful (and indeed appear to be inside the Pactor Modems)….they are limited in their ability to deal with multi-second strong interference that wipes out a long string of packets.

We would be back to the days when you were trying to download a file….**and when it finished, you were told it was corrupted.** With no ARQ, the failure to receive several packets would mean you are likely left with a corrupt or incomplete file.[41] If it includes important details for the life safety of persons in a shelter, what do you do then? Amateurs would be stuck with re-downloading the same message, possibly multiple times – and then trying to use UNIX tools to compare them and find what is missing. That seems to set amateur radio back by perhaps 40 years.

But the Filer's monitoring goals would also be seriously hindered. Were Filer's over-the-air FEC-only monitoring required, there would be no further impetus other than sheer goodwill for the WINLINK group to maintain their giant distributed-receiver web viewer, for which they have received such criticism from European amateurs. So that might go away – and searching 17,000 emails will no longer even be remotely possible in 5 minutes, as it is right now. Instead, the Filer will need to recruit a very large number of volunteers who will be able to keep their radios operating (assisted no doubt by computer control over the Internet) 24 hours a day, through lightning storms and power outages, to come even close to the same monitoring that the WINLINK group has already made work every moment of the day. I don't think this would be in the best interests of monitoring.

Sincerely,

/s/ Gordon L. Gibby MDKX4Z
15216 NW 41st Avenue
Newberry, FL 32669

EMAIL DISTRIBUTION LIST

Eric Burger	Eric.Burger@fcc.gov
Lisa Fowlkes	Lisa.Fowlkes@fcc.gov
Ajit Pai	Ajit.Pai@fcc.gov
Geoffrey Starks	geoffrey.starks@fcc.gov
Michael O'Rielly	mike.o'rielly@fcc.gov
Jessica Rosenworcel	Jessica.Rosenworcel@fcc.gov
Rachael Bender	Rachael.Bender@fcc.gov
Zenji Nakazawa	Zenji.Nakazawa@fcc.gov
Michael Wilhelm	Michael.Wilhelm@fcc.gov

41 Karn: "Far from being suited only to wireline communications, ARQ is essential to reliable communications. Contrary to Filer's claim, forward error correction (FEC) cannot guarantee reliability; it is merely an optional performance enhancement (though a very important one on radio channels). " in https://ecfsapi.fcc.gov/file/10513525129724/rm11831-rebuttal-to-rappaport.pdf

Curt Bartholomew	Curt.Bartholomew@fcc.gov
Erin McGrath	Erin.McGrath@fcc.gov
Brendan Carr	Brendan.Carr@fcc.gov
Julius Knapp	Julius.Knapp@fcc.gov
Michael Ha	michael.ha@fcc.gov
Ronald Repasi	Ronald.Repasi@fcc.gov
Bruce Jacobs	Bruce.Jacobs@fcc.gov
Donald Stockdale	Donald.Stockdale@fcc.gov
Roger Noel	Roger.Noel@fcc.gov
Scot Stone	Scot.Stone@fcc.gov
Rosemary Harold	Rosemary.Harold@fcc.gov
Charles Cooper	charles.cooper@fcc.gov
Laura Smith	Laura.Smith@fcc.gov